Claims

[c1] A method for protecting an item of content, comprising:
monitoring a plurality of file sharing networks to identify at least a first file sharing network having said item of content;
creating at least first and second reference files associated with said item of content, said first and second reference files each having a different format;
creating a plurality of decoy files, including a first set of decoy files created from said first reference file, and a second set of decoy files created from said second reference file, each of said decoy files including a defect; and
disseminating said decoy files to said first file sharing network.

[c2] The method of claim 1, further comprising causing a plurality of dissemination agents to register with said at least first file sharing network, and wherein said disseminating further includes causing said dissemination agents to disseminate said decoy files to said first file sharing network.

[c3] The method of claim 1, further comprising:
causing a plurality of query agents to register with said at least first file sharing network, and wherein said monitoring further includes causing said query agents to submit queries to said at least first file sharing network.

[c4] The method of claim 1, further comprising:
identifying a network syntax associated with said at least first file sharing network;
identifying a connectivity requirement associated with said at least first file sharing network; and
causing a plurality of agents to register with said at least first file sharing network using said network syntax and said connectivity requirement.

[c5] The method of claim 1, further comprising:
analyzing said first file sharing network to identify an effect of said disseminating.

[c6] The method of claim 5, wherein said analyzing further comprises:
comparing information about said first file sharing network to an expected

behavior model;
disseminating additional decoy files to said first file sharing network if said comparing indicates that said first file sharing network requires additional decoy files.

[c7] The method of claim 6, further comprising:
adjusting said expected behavior of dissemination model.

[c8] The method of claim 5, wherein said analyzing further comprises:
comparing information about said first file sharing network to an expected behavior model;
generating a third set of decoy files having different characteristics selected based on said comparing; and
disseminating decoy files from said third set to said first file sharing network.

[c9] The method of claim 1, further comprising:
causing a plurality of agents to register as users of said first file sharing network.

[c10] The method of claim 1, wherein said creating said reference files further comprises:
identifying a format associated with said first file sharing network; and
wherein at least one of said first and second reference files are created in said format associated with said first file sharing network.

[c11] The method of claim 1, wherein said creating said reference files further comprises:
identifying a plurality of alternative file formats associated with a media type of said item of content, wherein said first and second reference files are created based on said identified file formats.

[c12] The method of claim 1, wherein said creating said reference files further comprises:
identifying a plurality of alternative file formats associated with a media type of said item of content; and
creating a plurality of reference files from said item of content, each reference

file having a different one of said plurality of alternative file formats.

[c13] The method of claim 1, wherein said creating said reference files further comprises creating said reference files from a digital master copy of said item content.

[c14] The method of claim 1, wherein said monitoring further comprises:
identifying the number of said files on said first file sharing network.

[c15] The method of claim 14, wherein said identifying further comprises:
detecting at least one of an expected file name, a file size, a file format, a variant of said expected file name, a meta-descriptor, and a supplemental descriptor.

[c16] The method of claim 15, wherein said identifying further comprises:
performing a secondary identification process if said file can not be identified based on said detecting.

[c17] The method of claim 14, wherein the number of decoy files in said first and second sets is based on the number of said items of content on said first file sharing network.

[c18] The method of claim 14, wherein the number of decoy files in said first and second sets is selected to be sufficient to degrade performance of said first file sharing network.

[c19] The method of claim 1, wherein said monitoring further comprises:
querying each of said plurality of file sharing networks to identify a number of files matching any of said first and second reference files.

[c20] The method of claim 19, wherein each query is performed by an agent registered to participate in at least one of said plurality of file sharing networks.

[c21] The method of claim 1, wherein said creating a first set of decoy files further comprises
marking each of said decoy files with an identifier distinguishing said decoy files from said item of content.

[c22] The method of claim 21, wherein said identifier uniquely identifies said decoy to an entity creating said decoy, wherein said identifier is selected from the group consisting of: a digital watermark; a digital fingerprint; a hash; and a digital signature.

[c23] The method of claim 1, wherein said file is at least one of an audio file, a video file, an image, a software file, a text file and a data file, and said defect is selected from the group consisting of: a modification of one or more portions of the file; a repeating of portions of the file; a degradation of one or more portions of the file; a progressive degradation of portions of the file; and a modulation of a sampling rate of the file.

[c24] The method of claim 1, wherein said first set of decoy files includes at least a first and a second subset, wherein the decoy files in said first subset have a different defect that the decoy file in said second subset.

[c25] The method of claim 1, wherein said disseminating further comprises:
providing said first and second pluralities of decoy files to at least a first agent registered to participate in said first file sharing network; and
causing said agent to make said decoy files available to other users of said first file sharing network.

[c26] The method of claim 1, further comprising:
providing said first and second pluralities of decoy files to at least a first agent registered to participate in said first file sharing network;
providing said agent with dissemination instructions; and
causing said agent to make said decoy files available to other users of said first file sharing network pursuant to said dissemination instructions.

[c27] The method of claim 26, wherein said dissemination instructions include at least one of: a time of dissemination; a number of decoys to disseminate; and at least a first network variable.

[c28] The method of claim 1, wherein said creating said plurality of decoy files further comprises associating each of said decoy files with a validating characteristic.

[c29] The method of claim 28, wherein said validating characteristic is a hash function.

[c30] A method for protecting an item of content, comprising:
causing at least a first agent to register as a user of a file sharing network;
receiving data from said first agent identifying an unauthorized copy of said item of content, said unauthorized copy having a format;
creating a reference file based on said item of content in said format;
identifying a plurality of defects;
creating a plurality of decoy files from said reference file, each of said decoy files having one of said plurality of defects; and
causing said first agent to disseminate said plurality of decoy files using said file sharing network.